THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF UTAH

IN THE MATTER OF THE)
SEARCH OF:) 2:24-mj-00409 DBP
Item listed in Attachment A

SEALED AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Shenen P. Rose, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with Homeland Security Investigations (HSI), Office of the Assistant Special Agent-in-Charge in Salt Lake City, Utah. I have been employed as a Special Agent with HSI beginning in 2020 and I am currently assigned to investigate violations of federal law relating to child exploitation. Prior to employment HSI, I was employed in Federal Law Enforcement for twelve years, working as a Deportation Officer and Border Patrol Agent. While employed as a Deportation Officer, I was assigned as a Task Force Officer (TFO) with HSI and participated in child exploitation investigations and executed search warrants that resulted in the seizure of Child Sexual Abuse Material (CSAM). My education includes a Master of Science in Criminal Justice from Grand Canyon University and a Bachelor of Science in Criminal Justice from Utah Valley University. I have received training in the area of child pornography, child exploitation, and child sexual abuse and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. While employed by HSI, I have investigated Federal criminal violations related to child exploitation and child pornography, and the use of technology related to these types of criminal activity. Specifically, I have participated in numerous investigations relating to the sexual exploitation of children over the Internet.

2. Moreover, I am a Federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252, and 2252A, and is authorized by law to request a search warrant.

PURPOSE OF AFFIDAVIT

3. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search a cellphone (the "SUBJECT DEVICE"), more specifically described in **Attachment A** of this Affidavit, including the content of electronic storage located therein; and the content of any storage device therein, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251 (production of child pornography); 18 U.S.C. §§ 2252(a)(1), (b)(1) and 2252A (a)(1), (b)(1) (transportation of child pornography); 18 U.S.C. §§ 2252(a)(2), (b)(1) and 2252A(a)(2)(A), (b)(1) (receipt or distribution of child pornography); 18 U.S.C. §§ 2252(a)(4)(B), (b)(2) and 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) (the "Subject Offenses"), more specifically described in **Attachment B** of this Affidavit.

4. The statements in this affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the requested warrant.

BRIEF SUMMARY

5. As set forth in detail below, James Matthew MARSTON did possess images of Child Sexual Abuse Material. MARSTON's cellphones, the SUBJECT DEVICES, are currently in HSI custody. Child pornography can easily be accessed, viewed, downloaded, stored, and produced using the SUBJECT DEVICES. Thus, there is probable cause to search them for evidence, fruits, and instrumentalities of the Subject Offenses.

STATUTORY AUTHORITY

6. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting or shipping, or attempting or conspiring to transport or ship, any visual depiction using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer or mail, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction are of such conduct.

b. 18 U.S.C. § 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mail if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. 18 U.S.C. § 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

d. 18 U.S.C. § 2252A(a)(1) and (b)(1) prohibit a person from knowingly mailing, or transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography, as defined in 18 U.S.C. § 2256(8), or attempting or conspiring to do so.

e. 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

f. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. §

2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

7. The following definitions apply to this affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable

minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys,

which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Geolocated," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. A "hash value" is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

k. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an

IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

l. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

m. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

n. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

o. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

p. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an

electronic communications system.

q. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

r. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

s. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

PROBABLE CAUSE

8. On September 26, 2023, Detective Holly Coombs with Centerville Police Department received four referrals from the National Center for Missing and Exploited Children (NCMEC) regarding a Google user having up0loaded material to a user account which depicts the sexual exploitation of a minor. The related CyberTips (CT) are 173014882, 173115559, 173207509, 173305834.

9. NCMEC referral reads that on or about September 1, 2023, Google made a report that they had become aware of a user having uploaded contraband to the user's account. Google reported that they became aware of the issue either because they noticed it while reviewing files or because one or more of the uploaded files was a has match. The content, which contained 167 files, was stored in Google Photos infrastructure and Google Drive infrastructure.

10. Google LLC identified the suspect by Email address: sadclownbaddub187@gmail.com and two phone numbers, 801-661-3735 and 801-835-4079. Google LLC also captured several login and upload IP addresses. Google LLC also provided a "subscriber -data" pdf which showed all the IP addresses that were captured by Google LLC between August 5, 2023, at 01:20 hours (UTC) and September 1, 2023, at 5:51 hours (UTC), in regard to the Email address: sadclownbaddub187@gmail.com. Google confirmed the phone number 801-835-4079 on August 30, 2023, at 10:39:29 (UTC). As previously stated, based on the training and experience of Det. Coombs, when a provider such as Google "confirms" a phone number, they typically send a text message or make a phone call to the phone number to confirm that the phone number belongs to the account owner. Therefore, it is probable that the owner of the target email address used to access the CSAM belongs to the owner of phone number 801-835-4079.

11. Google provided the file titled "6473e2c2034645a487c907f1270012e9-Pretzels_6_-_Time_for_shower_is_time_to_play.mpg" which they stated they had viewed, determining it to be CSAM. Det. Coombs viewed the file, which is a 15 minute 1 second video of a prepubescent female in a bathroom initially wrapped in a bath towel. She removes the bath towel and exposes her genitals to the camera; she then proceeds to masturbate. She then gets into the shower. When she gets out of the shower, she wraps herself in the bath towel and stands over the camera exposing her genitals again.

12. There are multiple IP addresses used to login to this account, which Det. Coombs verified through Maxmind.com that geolocate to Utah. In addition to the IP addresses used to login to the account, the phone numbers associated with the Google account have a Utah area code.

13. When using an investigative tool to locate the owner of the phone number 801-835-4079, Det. Coombs found that it belonged to James MARSTON. Det. Coombs located a Utah driver's license #17803600, for MARSTON. Along with MARSTON's driver's

license, Det. Coombs found MARSTON was on parole and is a registered sex offender. Det. Coombs checked the Utah sex offender database, Offender Watch, and found the phone number provided to Adult Probation and Parole to be the same as reported in the CT, 801-835-4079.

14. Det. Coombs further found MARSTON was residing at 646 N. Gramercy, in Ogden, Utah. Additional checks conducted by Det Coombs through Offender Watch, showed MARSTON to have a new address of 1539 S. Burton Ct. This information was reported by MARSTON to his parole officer on October 16, 2023.

15. MARSTON's parole office, Bryan Lythgoe, confirmed to Det. Coombs that he had made a successful home visit with MARSTON at the Burton Ct. address in November of 2023.

16. On December 7, 2023, Det. Coombs along with the Utah Attorney General's Office Internet Crimes Against Children (ICAC) taskforce served a residential search warrant at the Burton Ct. residence of MARSTON.

17. Prior to serving the search warrant, Det Coombs also reached out to Agent Lythgoe, who was MARSTON's parole agent, who requested that Det. Coombs and the ICAC taskforce conduct a concurrent parole search of MARSTON's residence and electronic devices in accordance with MARSTON's parole agreement and terms of parole.

18. During the search of the residence, taskforce members located and seized two cellphones, a black Samsung cellphone (DEVICE 1) and a Black iPhone (DEVICE 2), herein and after referred to as SUBJECT DEVICES, belonging to MARSTON.

19. On December 11, 2023, Det. Coombs took the SUBJECT DEVICES to the Utah Attorney General's Office to be forensically examined. On December 19, 2023, Det. Coombs received the extraction reports from the Utah Attorney General's office and returned the SUBJECT DEVICES to Centerville Police Department for safekeeping.

20. Det. Coombs found in an extraction report, DEVICE 1 contained 182 files of

confirmed CSAM. These files were submitted to the National Center for Missing and Exploited Children (NCMEC) for hash value comparison. NCMEC report #140603-2024-HC identified the files contained 48 previously identified CSAM victims, 8 recognized hash values, and 126 unrecognized hash values.

21. The extraction report of DEVICE 2, showed only a partial extraction was completed and no CSAM was found in that extraction. Based on my training and experience, and conversations with other law enforcement, a partial extraction is often the result of not having a passcode for the device and/or the tools used to conduct the extraction are not update to the software installed on the affected device. Frequent updates to forensic tools have led to devices being able to be fully extracted after an initial extraction failure or incomplete extraction.

22. In February of 2024, I was notified about this investigation and asked to provide assistance in further investigating for Child Sexual Abuse Material in SUBECT DEVICES.

23. As part of my investigation, I believe it would be beneficial for a Forensic Analyst at Homeland Security Investigations to re-examine the SUBJECT DEVICES data in this case. I know from training and experience that investigators use a variety of tools and techniques to investigate the contents of computers and cell phones. I know that the investigative tools are updated from time to time which can result in additional data that resides on a device being made available to an examiner who conducts a new extraction from the device. I also know that different tools created by different companies or agencies may have increased or decreased ability to read data that resides on a device. I also know that the investigative strategies and techniques employed by forensic examiners may allow for the identification of different evidence as the data is searched.

24. Based on my training and experience, the data that exists on cellular devices, computers, or the extraction of a digital device will remain until deleted. Because no one has had access to the SUBJECT DEVICES since they were seized from MARSTON, I believe that the

digital data that existed on the SUBJECT DEVICES at the time of MARSTON's arrest will still reside on the SUBJECT DEVICES.

25. Although a warrant was already obtained to search the SUBJECT DEVICES, the information obtained from service of the prior warrant has recovered evidence of CSAM and with the update of technology, a new forensic examination of the subject DEVICES is likely to reveal additional evidence of CSAM.

26. I also know that people who use child pornography often have multiple DEVICES, such as multiple cellphones, in order to conceal their consumption of child pornography from law enforcement and/or family members. Often people involved in criminal conduct will have a fully functional cellphone they use publicly and provide it is their primary phone without disclosing the use of an additional phone that can be used to store illegal files or access internet via WiFi to view illegal content such as child exploitation material.

27. Further, I know that suspects in these criminal cases sometimes claim that the DEVICE was not in their possession during the time child pornography was accessed. Collateral clues that can be discovered through observing what other activity was taking place on the device at or around the time the child pornography was accessed is critical in showing the identity of the person who accessed the child pornography. Correspondence such as emails or text messages at or around the time that the child pornography was being accessed is therefore relevant to show that the suspect was the person who controlled the child pornography.

28. Because child pornography can be difficult to find or obtain, I know from training and experience that people who produce child pornography are often involved in distributing that child pornography to other individuals. Sometimes this distribution is done to facilitate the collection of additional child pornography in a "trade" of child pornography material. Other times produced child pornography is distributed in exchange for money or other valuable consideration. Still other times, child pornography is distributed in

exchange for attention or affection from others.

29. Based on the facts and opinions detailed in this affidavit, specifically information reported by Det. Coombs, I believe there are visual depictions of CSAM contained in the SUBJECT DEVICES.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

30. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer

itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other likeminded offenders or with potential minor victims, and to access cloud-storage

services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

31. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT DEVICES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

32. I submit that there is probable cause to believe those records referenced above will be stored on the SUBJECT DEVICES, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer

files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

33. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that there is forensic electronic evidence stored on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a

file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such

information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the

application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

34. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer

equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a

"dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

35. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, andwould authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. These searches are conducted with the aid of software and techniques which are continually evolving. As such, as investigators uncover new techniques to search a device and as software is updated, future searches are likely to uncover additional evidence. As such, it is requested this warrant will allow for repeated forensic review up to and including the time of trial.

CONCLUSION

36. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits, and instrumentalities of the SUBJECT offenses, more fully described in Attachment B, are located on the SUBJECT DEVICES described in Attachment A. I respectfully request that this Court issue a search warrant for the DEVICES described in Attachment A, authorizing the seizure and Search of the items described in Attachment

B. It is intended this warrant will allow for off-site forensic review up to and including the time of trial.

37. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

SHENEN P ROSE Digitally signed by SHENEN P ROSE Date: 2024.04.17 05:24:42 -06'00'

/s/ Shenen P. Rose
Shenen P. Rose
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 17 th day of April, 2024.

United States Magistrate Judge

United States District Court District of Utah

ATTACHMENT A

DESCRIPTION OF DEVICE TO BE SEARCHED

The devices to be searched, which are currently in possession of Homeland Security Investigations at 2975 Decker Lake Drive, West Valley City, UT 84119, in the District of Utah, are:

DEVICE 1: Black Samsung cellphone seized from James Matthew MARSTON pursuant to a State of Utah Search Warrant.

DEVICE 2: Black iPhone seized from James Matthew MARSTON pursuant to a State of Utah Search Warrant.

ATTACHMENT B

ITEMS TO BE SEIZED

The items to be seized, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely 18 U.S.C. § 2251 (production of child pornography); 18 U.S.C. §§ 2252(a)(1), (b)(1) and 2252A (a)(1), (b)(1) (transportation of child pornography); 18 U.S.C. §§ 2252(a)(2), (b)(1) and 2252A(a)(2)(A), (b)(1) (receipt or distribution of child pornography); 18 U.S.C. §§ 2252(a)(4)(B), (b)(2) and 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) (the "Subject Offenses"), are:

1. SUBJECT DEVICES and any storage device contained therein if used as a means to commit the SUBJECT OFFENSES.

2. For each SUBJECT DEVICE, including any storage device contained therein:

   a. evidence tending to identify who used, owned, or controlled the DEVICE at the time the things described in this warrant were created, edited, or deleted, such logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

   b. evidence of software that would allow others to control the DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   c. evidence of the lack of such malicious software;

   d. evidence indicating how and when the DEVICE was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the DEVICE user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the DEVICE of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the DEVICE;

h. evidence of the times the DEVICE was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the DEVICE;

j. documentation and manuals that may be necessary to access the DEVICE or to conduct a forensic examination of the DEVICE;

k. records of or information about Internet Protocol addresses used by the DEVICE;

l. records of or information about the DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica (material that may not legally be child pornography but nevertheless appeals to the sexual interest of individuals who are sexually interested in minors; child erotica could be visual depictions, drawings, artwork, stories, etc).

4. Any material, in any form, tending to identify any individual involved in the Subject Offenses or otherwise involved in the sexual exploitation of minors;

5. Any material, in any form, tending to identify any minor who is, or appears to be, the victim the Subject Offenses or the sexual exploitation of minors;

6. Any material, in any form, tending to identify the means or methods used to commit the Subject Offenses;

7. All saved "chat" or messaging transcripts related to the Subject Offenses including but limited to any material reflecting a sexual interest in children or the sexual exploitation of minors;

8. Any material, in any form, pertaining to child pornography, child erotica, an interest in such materials, or pertaining to a sexual interest in children, or sexual activity involving children;

9. Any material, in any form, tending to identify the user of the SUBJECT DEVICE;

10. Content of web history and searches related to the SUBJECT OFFENSES or otherwise reflect a sexual interest in children or images of children;

11. Location information associated with the SUBJECT DEVICE listed in Attachment A that tends to identify the user of the DEVICE, events relating to the Subject Offenses, assist in the determinate of the chronological and geographic context of the Subject Offenses, tends to show where events occurred, and who sent, received, possessed or produced child pornography or other evidence of the Subject Offenses;

12. EXIF or other metadata about images, documents or correspondence related to the Subject Offenses, reflecting a sexual interest in children, or that help identify the device or person who produced, sent, traded, received, or possessed child pornography or that identifies the user of the accounts used to engage in child exploitative acts.

13. Any material, in any form, concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members, advertise, promote, discuss or otherwise involve child pornography, or otherwise relate to the Subject Offenses or the sexual exploitation of children;

14. Any material, in any form, pertaining to the means and source of payment for services related to the Subject Offenses, such as payment for messaging applications, internet services, website access, child pornography, (including any credit card or bank account number or digital money transfer account information or payment for gaming services);
15. Any material, in any form, tending to evidence CRAIG's state of mind as it relates to the Subject Offenses;

16. Any material, in any form, tending to identify digital devices owned, used, controlled or accessed by CRAIG, including but not limited to the SUBJECT DEVICE;

17. Definitions for terms as used herein:

    a. The terms "materials," "records" "information" and "evidence" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data;

    b. The term "computer" or "device" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

1. As described above and in Attachment B, this warrant allows law enforcement to search for records that might be found on the SUBJECT DEVICES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

2. There is probable cause to believe those records referenced above will be stored on the SUBJECT DEVICES, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations,

artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

3. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and

prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates

to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. When an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of

crime. A computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

4. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. During the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if

certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

5. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, routers, modems,

and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

6. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.